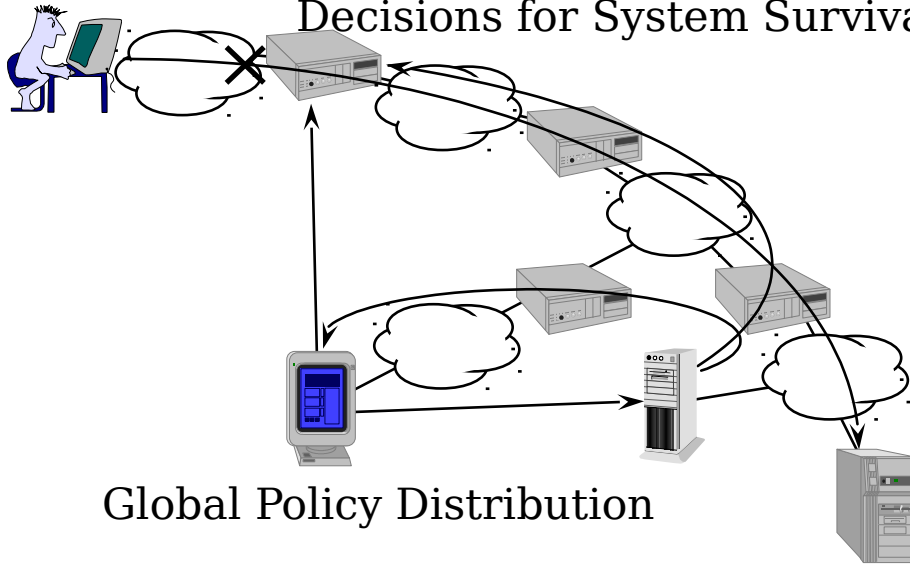


Adaptive System Security Policies

Intrusion Response in Networked Systems
Optimized Containment/Monitoring
Decisions for System Survivability



NEW IDEAS

- Extensions to the Intruder Detection and Isolation Protocol (IDIP) to enable adaptable response decisions that optimize system survivability
- Support for both local and global policies for intrusion response
- Integration of control capabilities and global policy management into the discovery coordinator

IMPACT

- Optimized survivability to network-based attacks
- Improved protection from insider attacks
- Support for network-wide intrusion response

SCHEDULE

Proof of Concept
Demonstration

1997	1998	1999
Adaptive Policies Defines		System-Level Demonstration